UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,025	08/16/2006	Wiebe De Haan	NL040228	9339

24737 7590 04/06/2010

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
CHANG, KENNETH W	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
04/06/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/598,025	DE HAAN ET AL.	
	Examiner	Art Unit	
	Kenneth Chang	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18,20,21 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18,20,21 and 23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The following is a Final Office action in response to communications received on 11/17/2009. Claims 1, 11, 13-18, 20, 21, and 23 have been amended. **Claims 1-18, 20, 21, and 23** are pending and have been considered as follows.

Response to Arguments

1. **As to Claims 1-18, 20, 21, and 23**, Applicants' amendment of independent Claims 1, 11, 13-18, 20, 21, and 23 necessitated a new ground(s) of rejection in this Office action. Therefore, Applicants' arguments filed on 11/17/2009 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. **Claims 1-5, 7, 8, 10-18, 20, 21, and 23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi et al. (US-20010042252-A1, hereinafter Yamaguchi) in view of Coupe et al. (US-20020064189-A1, hereinafter Coupe), and in further view of Raike (US-20020025045-A1).

As to Amended Claim 1:

Yamaguchi discloses a method of encrypting a data stream comprising at least one stream of audiovisual data (e.g. see "the present invention aims to provide a digital broadcast receiving device, a digital broadcast system, and a recording medium storing a receiving method and a receiving program, all of which can restrict use of interactive data relating to a fee-based program during a preview time" [0015]), comprising steps of,

- segmenting at least one of said at least one stream (MPEG2 transport stream [0063]) of audiovisual data into data segments (components [0066]) (e.g. see "The sending device 20 is installed in a broadcast station that provides a digital broadcast service, and sends an MPEG2 (Moving Picture Expert Group) TP (transport stream) as a broadcast wave via the broadcast satellite 30… The reception signal is composed of video data, audio data, interactive data" [0063]; see also "When transmitted, the MPEG2 TS 200 is divided into packets on a transmission channel. Each packet contains a different packet ID (PID), which is identification information for the packet" [0065]);
- providing the data segments with ID data (component ID [0066]) in an ID segment (MPEG2 TS 200 packet headers [0065]-[0066]), the ID data being

[different from] ID data being pre-determined (packet id, PID [0065]) to identify the type of data (audio, video, or interactive data [0063]) in the stream of audiovisual data (e.g. see "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure. Each component contains a different component ID that identifies the component" [0066]; see also "The component 217 includes viewing permission information 218, which contains subscription information given for each program... Video data and audio data are included in a video data component and an audio data component, which are not shown in the figure" [0067]; see also "Each reception element has a different reception element ID to identify the reception element, and each presentation element has a different presentation ID to identify the presentation element" [0070]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized;
- partly encrypting the data segments, leaving the ID segment unencrypted (although Yamaguchi does disclose "Encryption (hereafter, "scrambling") is performed separately for each TP (hereafter, "AV (audio-video) TP" [Transport Packets]) containing video data and audio data for programs" [0008]).

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]) such that the altered ID data (i.e. null PID [0062])

renders the type of data in the at least one stream unrecognized (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded). Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data packet streams, does disclose partly encrypting the data segments (encrypting packet payload [0035]), leaving the ID segment (packet header information with ID tag [0029] and [0035]) unencrypted.

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table 230 comprises a programmable PID look-up table having n entries, wherein in one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);
- (e.g. see Raike, "The present encryption processing may insert specific information into designated field(s) within the stream header, and also replaces the data payload of each packet with encrypted data. All of the packets in the stream are encrypted, but only the data payload is encrypted and not the packet

header information. This remains unchanged by the encryption processing" [0035]; see also "each packet header is assumed to include at least one item of information that uniquely identifies that packet, called here a "tag"... The tag information, along with the rest of the packet header, must accompany a packet "in the clear", that is, not encrypted" [0029]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe and Raike to include an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized and partly encrypting the data segments, leaving the ID segment unencrypted as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to designate and discard certain data stream packets (Coupe [0062]) and facilitating the encryption and decryption of the data packets (Raike [0032]-[0035]).

As to Claim 2:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 1, wherein the method further comprises the step of,

- creating data packs (components, Yamaguchi [0066]), each data pack comprising at least one data segment (packets [0065]) and wherein the step of partly encrypting the data segments, the ID segment (packet header information

with ID tag, Raike [0029] and [0035]) of said at least one data segment is unencrypted (e.g. see Yamaguchi, "A plurality of packets that has the same PID to be transmitted make up the same component" [0065]; see also "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure" [0066]; see also Raike, "The present encryption processing may insert specific information into designated field(s) within the stream header, and also replaces the data payload of each packet with encrypted data. All of the packets in the stream are encrypted, but only the data payload is encrypted and not the packet header information. This remains unchanged by the encryption processing" [0035]);

- The examiner supplies the same rationale for the combination of references Yamaguchi, Coupe, and Raike as in claim 1 above.

As to Claim 3:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 1, wherein the at least one data stream comprises,

- multiple streams of different types of audiovisual data and data segments of at least one stream of audiovisual data are encrypted (e.g. see Yamaguchi, "For this communication satellite broadcast service, a plurality of transport streams (hereafter called "TS") for digital data are broadcasted in parallel. The number of transport streams broadcasted in parallel is equal to a number of transponders. A plurality of transport packets (hereafter "TP"), which contain data corresponding to a plurality of programs, are time-division multiplexed into each TS. A user

selects a given program contained in a TS, and watches the program" [0006]; see also “Encryption (hereafter, "scrambling") is performed separately for each TP (hereafter, "AV (audio-video) TP") containing video data and audio data for programs" [0008]).

As to Claim 4:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 3, wherein,

- data segments of at least one stream of audiovisual data is provided with ID segments (MPEG2 TS 200 packet headers, Yamaguchi [0065]-[0066]) comprising ID data (component ID [0066]) being different from ID data being pre-determined to identify the type of data in the stream of audiovisual data (e.g. see Yamaguchi, “As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure. Each component contains a different component ID that identifies the component" [0066]; see also “The component 217 includes viewing permission information 218, which contains subscription information given for each program… Video data and audio data are included in a video data component and an audio data component, which are not shown in the figure" [0067]).

As to Claim 5:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 3, wherein,

- the multiple streams of different types of audiovisual data are provided simultaneously and the method further comprising the step of multiplexing the segments comprising data of the multiple streams of audiovisual data to a further data stream (e.g. see Yamaguchi, "A plurality of transport packets (hereafter "TP"), which contain data corresponding to a plurality of programs, are time-division multiplexed into each TS. A user selects a given program contained in a TS, and watches the program" [0006]; see also "The combining unit 106 receives the second AV signal from the AV reproducing unit 105, and a second data signal from the data analyzing unit 104. The combining unit 106 then combines the second AV signal and the second data signal to generate a data-AV combined signal, and outputs the generated data-AV combined signal to the monitor connected to the interactive data receiving device 100" [0108]).

As to Claim 7:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 2, wherein,

- the data packs are MPEG-2 data stream packs (e.g. see Yamaguchi, "The sending device 20 is installed in a broadcast station that provides a digital broadcast service, and sends an MPEG2 (Moving Picture Expert Group) TP (transport stream) as a broadcast wave via the broadcast satellite 30" [0063]; see also "When transmitted, the MPEG2 TS 200 is divided into packets on a transmission channel" [0065]).

As to Claim 8:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 1, wherein,

- the ID data being pre-determined to identify the type of data in the stream of audiovisual data is pre-determined by the DVD standard (e.g. see Yamaguchi, "The sending device 20 is installed in a broadcast station that provides a digital broadcast service, and sends an MPEG2 (Moving Picture Expert Group) TP (transport stream) as a broadcast wave via the broadcast satellite 30" [0063]; see also "When transmitted, the MPEG2 TS 200 is divided into packets on a transmission channel. Each packet contains a different packet ID (PID), which is identification information for the packet" [0065] where the DVD standard inherently uses the MPEG2 format in its specification).

As to Claim 10:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 1, further comprising,

- storing the segmented and partially encrypted data segments on a storage medium (e.g. see Yamaguchi, "In view of the above problems, the present invention aims to provide a digital broadcast receiving device, a digital broadcast system, and a recording medium storing a receiving method and a receiving program, all of which can restrict use of interactive data relating to a fee-based program during a preview time" [0015]; see also "The data storing unit 108 is composed of semiconductor memory, and has areas that store a presentation

element, a purchase state, a component ID, a reception element ID, and a presenting element flag, as shown in FIG. 5" [0088]).

As to Amended Claim 11:

Yamaguchi discloses a circuit (sending device 20 [0061]) for encrypting a data stream comprising at least one stream of audiovisual data, comprising (see Applicant Spec. Page 11 lines 8-9, "For example, a function being described as being carried out by one element may also be carried out by multiple elements and vice versa [multiple functions carried out by one element]"),

- a segmenting unit (sending device 20's processor) for segmenting the stream of audiovisual data in data segments (e.g. see "The sending device 20 is installed in a broadcast station that provides a digital broadcast service, and sends an MPEG2 (Moving Picture Expert Group) TP (transport stream) as a broadcast wave via the broadcast satellite 30" [0063]; see also "When transmitted, the MPEG2 TS 200 is divided into packets on a transmission channel" [0065] where sending device 20 inherently uses a processor for these functions);
- a unit (sending device 20's processor) for providing the data segment with ID data (component ID [0066]) in an ID segment (MPEG2 TS 200 packet headers [0065]-[0066]), the ID data [different from] ID data (packet id, PID [0065]) being pre-determined to identify the type of data in the stream of audiovisual data (e.g. see "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure. Each component contains a different component ID that identifies the component"

[0066]; see also "The component 217 includes viewing permission information 218, which contains subscription information given for each program... Video data and audio data are included in a video data component and an audio data component, which are not shown in the figure" [0067]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized;
- an encryption unit for partly encrypting the data segments, leaving the ID segment unencrypted (although Yamaguchi does disclose "Encryption (hereafter, "scrambling") is performed separately for each TP (hereafter, "AV (audio-video) TP" [Transport Packets]) containing video data and audio data for programs" [0008]).

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]) such that the altered ID data (i.e. null PID [0062]) renders the type of data in the at least one stream unrecognized (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded). Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data streams, does disclose an encryption unit (sender's encryption processor [0005]) for partly encrypting the data segments (encrypting packet payload [0035]), leaving the ID segment (packet header information with ID tag [0029] and [0035]) unencrypted.

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table 230 comprises a programmable PID look-up table having n entries, wherein in one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);
- (e.g. see Raike, "The present encryption processing may insert specific information into designated field(s) within the stream header, and also replaces the data payload of each packet with encrypted data. All of the packets in the stream are encrypted, but only the data payload is encrypted and not the packet header information. This remains unchanged by the encryption processing" [0035]; see also "each packet header is assumed to include at least one item of information that uniquely identifies that packet, called here a "tag"... The tag information, along with the rest of the packet header, must accompany a packet "in the clear", that is, not encrypted" [0029]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe

and Raike to include an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized and an encryption unit for partly encrypting the data segments, leaving the ID segment unencrypted as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to designate and discard certain data stream packets (Coupe [0062]) and facilitating the encryption and decryption of the data packets (Raike [0032]-[0035]).

As to Claim 12:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the circuit according to claim 11, further comprising,

- a packing unit (sending device 20's processor) for creating data packs (components, Yamaguchi [0066]), each data pack comprising at least one data segment (packets [0065]) and wherein the step of partly encrypting the data segments, the ID segment (packet header information with ID tag, Raike [0029] and [0035]) of said at least one data segment is unencrypted (e.g. see Yamaguchi, "A plurality of packets that has the same PID to be transmitted make up the same component" [0065]; see also "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure" [0066]; see also Raike, "The present encryption processing

may insert specific information into designated field(s) within the stream header, and also replaces the data payload of each packet with encrypted data. All of the packets in the stream are encrypted, but only the data payload is encrypted and not the packet header information. This remains unchanged by the encryption processing" [0035]);

- The examiner supplies the same rationale for the combination of references Yamaguchi, Coupe, and Raike as in claim 11 above.

As to Amended Claim 13:

Yamaguchi discloses an apparatus (FIG. 1, interactive data receiving devices 100a and 100b) for storing data, comprising,

- a receiver for receiving data (e.g. see "As shown in FIG. 4, the interactive data receiving device 100 includes a receiving unit 101" [0086]);
- the circuit comprising:
- a segmenting unit (sending device 20's processor) for segmenting the stream of audiovisual data in data segments (e.g. see "The sending device 20 is installed in a broadcast station that provides a digital broadcast service, and sends an MPEG2 (Moving Picture Expert Group) TP (transport stream) as a broadcast wave via the broadcast satellite 30" [0063]; see also "When transmitted, the MPEG2 TS 200 is divided into packets on a transmission channel" [0065] where sending device 20 inherently uses a processor for these functions);
- a unit (sending device 20's processor) for providing the data segment with ID data (component ID [0066]) in an ID segment (MPEG2 TS 200 packet headers

[0065]-[0066]), the ID data [different from] ID data (packet id, PID [0065]) being pre-determined to identify the type of data in the stream of audiovisual data (e.g. see "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure. Each component contains a different component ID that identifies the component" [0066]; see also "The component 217 includes viewing permission information 218, which contains subscription information given for each program... Video data and audio data are included in a video data component and an audio data component, which are not shown in the figure" [0067]);

- a storage device (data storing unit) for storing partially encrypted data segments on a storage medium (e.g. see "The data storing unit 108 is composed of semiconductor memory, and has areas that store a presentation element, a purchase state, a component ID, a reception element ID, and a presenting element flag, as shown in FIG. 5" [0088]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized;
- an encryption unit for partly encrypting the data segments, leaving the ID segment unencrypted (although Yamaguchi does disclose "Encryption (hereafter, "scrambling") is performed separately for each TP (hereafter, "AV (audio-video) TP" [Transport Packets]) containing video data and audio data for programs" [0008]).

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]) such that the altered ID data (i.e. null PID [0062]) renders the type of data in the at least one stream unrecognized (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded). Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data streams, does disclose an encryption unit (sender's encryption processor [0005]) for partly encrypting the data segments (encrypting packet payload [0035]), leaving the ID segment (packet header information with ID tag [0029] and [0035]) unencrypted.

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table 230 comprises a programmable PID look-up table having n entries, wherein in one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);

- (e.g. see Raike, "The present encryption processing may insert specific information into designated field(s) within the stream header, and also replaces the data payload of each packet with encrypted data. All of the packets in the stream are encrypted, but only the data payload is encrypted and not the packet header information. This remains unchanged by the encryption processing" [0035]; see also "each packet header is assumed to include at least one item of information that uniquely identifies that packet, called here a "tag"... The tag information, along with the rest of the packet header, must accompany a packet "in the clear", that is, not encrypted" [0029]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe and Raike to include an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized and an encryption unit for partly encrypting the data segments, leaving the ID segment unencrypted as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to designate and discard certain data stream packets (Coupe [0062]) and facilitating the encryption and decryption of the data packets (Raike [0032]-[0035]).

As to Amended Claim 14:

Yamaguchi discloses a method of decrypting audiovisual data (e.g. see "the present invention aims to provide a digital broadcast receiving device, a digital broadcast system, and a recording medium storing a receiving method and a receiving program, all of which can restrict use of interactive data relating to a fee-based program during a preview time" [0015]), comprising the steps of,

- recognising that the data carried by the ID segment is [different from] ID data being pre-determined to identify the type of data in the stream of audiovisual data and recognising the actual type of data comprised by the data segments (e.g. see "The data judging unit 117 then compares the ID of the recognized link destination with the ID of the currently-presented presentation element to judge whether a presentation element of the link destination and the currently-presented presentation element belong to the same component" [0126]);
- forming a stream of audiovisual data from the data segments (e.g. see "The combining unit 106 receives the second AV signal from the AV reproducing unit 105, and a second data signal from the data analyzing unit 104. The combining unit 106 then combines the second AV signal and the second data signal to generate a data-AV combined signal, and outputs the generated data-AV combined signal to the monitor connected to the interactive data receiving device 100" [0108]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data, wherein the data is unrecognized;

- decrypting the partly encrypted data segments (although Yamaguchi discloses "A descrambling key to descramble such scrambled AV TP [audio-video transport packets], and program attribute information for the programs make up program information (hereafter, "ECM") and are contained in another TP (hereafter, "ECM TP"). Such ECM TP and AV TP are broadcasted together. This ECM TP is also scrambled. A work key to descramble the scrambled ECM TP, and subscription information make up individual information (hereafter, "EMM") and are stored in an integrated circuit (IC) card, which is inserted into each receiving device" [0008]);

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]), wherein the data is unrecognized (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded). Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data streams, does disclose decrypting (symmetrically decrypting [0034]) the partly encrypted data segments (encrypted stream packets with unencrypted tag values removed [0034]).

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table

230 comprises a programmable PID look-up table having n entries, wherein in one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);

- (e.g. see Raike, "The tag values of each stream data packet are extracted (13) and then hashed (14) with the base key to produce the packet key for each packet. The stream packets with tag values removed (stream data) are then symmetrically decrypted (15) using the corresponding packet key. The plaintext stream packets, with or without tag values depending on the transmission protocol being used, are then stored or outputted in a form suitable for use by a streaming media player" [0034]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe and Raike to include an alteration of ID data, wherein the data is unrecognized and decrypting the partly encrypted data segments as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to

designate and discard certain data stream packets (Coupe [0062]) and facilitating the later decryption process of the encrypted stream packets (Raike [0032]-[0035]).

As to Amended Claims 15, 16, and 17:

Yamaguchi discloses a method/circuit/apparatus for decrypting audiovisual data, retrieving and rendering stored audiovisual data (e.g. see "the present invention aims to provide a digital broadcast receiving device, a digital broadcast system, and a recording medium storing a receiving method and a receiving program, all of which can restrict use of interactive data relating to a fee-based program during a preview time" [0015]), comprising,

- a storage device for/retrieving data stored on a storage medium (e.g. see "The receiving unit 101 receives an MPEG2 TS (hereafter, "TS"), which is transmitted repeatedly from the sending device 20 as a broadcast wave, and extracts a reception signal and viewing permission information from the received TS. This reception signal contains video data, audio data, and interactive data. The receiving unit 101 then outputs the extracted reception signal to the restoring unit 103, and the extracted viewing permission information to the specifying unit 102" [0097]);
- an identification unit for/recognizing that the data carried by the ID segment is [different from] ID data (data judging unit 117 distinguishes ID data such as a component ID from a packet ID) being pre-determined to identify the type of data in the stream of audiovisual data (e.g. see "The data judging unit 117 then compares the ID of the recognized link destination with the ID of the currently-

presented presentation element to judge whether a presentation element of the link destination and the currently-presented presentation element belong to the same component" [0126]);

- a streaming unit for/forming a stream of audiovisual data from the data segments (e.g. see "The combining unit 106 receives the second AV signal from the AV reproducing unit 105, and a second data signal from the data analyzing unit 104. The combining unit 106 then combines the second AV signal and the second data signal to generate a data-AV combined signal, and outputs the generated data-AV combined signal to the monitor connected to the interactive data receiving device 100" [0108]);
- a circuit for/rendering the decrypted stream of audiovisual data (e.g. see "When the purchase state signal indicates the preview state (step S301), the data analyzing unit 104 generates video data, which is a second data signal, referring to a bitmap table, a text table, and the like included in a firstly-presented presentation element (step S304), and outputs the generated second data signal to the combining unit 106 (step S305). The processing is then completed" [0207]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data and not recognising the actual type of data comprised by the data segments based on the altered ID data;
- a decryption unit for/decrypting the partly encrypted data segments (although Yamaguchi discloses "A descrambling key to descramble such scrambled AV TP

[audio-video transport packets], and program attribute information for the programs make up program information (hereafter, "ECM") and are contained in another TP (hereafter, "ECM TP"). Such ECM TP and AV TP are broadcasted together. This ECM TP is also scrambled. A work key to descramble the scrambled ECM TP, and subscription information make up individual information (hereafter, "EMM") and are stored in an integrated circuit (IC) card, which is inserted into each receiving device" [0008]);

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]), and not recognizing the actual type of data comprised by the data segments based on the altered ID data (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded). Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data streams, does disclose a decryption unit (recipient's decryption processor [0030]) for/decrypting (symmetrically decrypting [0034]) the partly encrypted data segments (encrypted stream packets with unencrypted tag values removed [0034]).

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table 230 comprises a programmable PID look-up table having n entries, wherein in

one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);

- (e.g. see Raike, "The tag values of each stream data packet are extracted (13) and then hashed (14) with the base key to produce the packet key for each packet. The stream packets with tag values removed (stream data) are then symmetrically decrypted (15) using the corresponding packet key. The plaintext stream packets, with or without tag values depending on the transmission protocol being used, are then stored or outputted in a form suitable for use by a streaming media player" [0034]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe and Raike to include an alteration of ID data and not recognising the actual type of data comprised by the data segments based on the altered ID data and a decryption unit for/decrypting the partly encrypted data segments as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to

designate and discard certain data stream packets (Coupe [0062]) and facilitating the later decryption process of the encrypted stream packets (Raike [0032]-[0035]).

As to Amended Claims 18 and 20:

Yamaguchi discloses a computer programme product/programmed computer comprising computer readable instruction for programming a processing unit (e.g. see "The present invention may be a computer system that comprises a microprocessor and memory which stores the above computer program, and the microprocessor may execute the stored computer program to achieve the present invention. The above computer program or digital signals may be recorded on the computer-readable recording medium to be distributed via the network or other distribution methods to a computer system" [0258]), enabled to execute the steps of,

- segmenting at least one of said at least one stream (MPEG2 transport stream [0063]) of audiovisual data in data segments (components [0066]) (e.g. see "The sending device 20 is installed in a broadcast station that provides a digital broadcast service, and sends an MPEG2 (Moving Picture Expert Group) TP (transport stream) as a broadcast wave via the broadcast satellite 30… The reception signal is composed of video data, audio data, interactive data" [0063]; see also "When transmitted, the MPEG2 TS 200 is divided into packets on a transmission channel. Each packet contains a different packet ID (PID), which is identification information for the packet" [0065]);
- providing the data segments with ID data (component ID [0066]) in an ID segment (MPEG2 TS 200 packet headers [0065]-[0066]), the ID data being

[different from] ID data being pre-determined (packet id, PID [0065]) to identify the type of data (audio, video, or interactive data [0063]) in the stream of audiovisual data (e.g. see "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure. Each component contains a different component ID that identifies the component" [0066]; see also "The component 217 includes viewing permission information 218, which contains subscription information given for each program... Video data and audio data are included in a video data component and an audio data component, which are not shown in the figure" [0067]; see also "Each reception element has a different reception element ID to identify the reception element, and each presentation element has a different presentation ID to identify the presentation element" [0070]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized;
- partly encrypting the data segments, leaving the ID segment unencrypted (although Yamaguchi does disclose "Encryption (hereafter, "scrambling") is performed separately for each TP (hereafter, "AV (audio-video) TP" [Transport Packets]) containing video data and audio data for programs" [0008]).

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]) such that the altered ID data (i.e. null PID [0062])

renders the type of data in the at least one stream unrecognized (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded). Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data packet streams, does disclose partly encrypting the data segments (encrypting packet payload [0035]), leaving the ID segment (packet header information with ID tag [0029] and [0035]) unencrypted.

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table 230 comprises a programmable PID look-up table having n entries, wherein in one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);
- (e.g. see Raike, "The present encryption processing may insert specific information into designated field(s) within the stream header, and also replaces the data payload of each packet with encrypted data. All of the packets in the stream are encrypted, but only the data payload is encrypted and not the packet

header information. This remains unchanged by the encryption processing" [0035]; see also "each packet header is assumed to include at least one item of information that uniquely identifies that packet, called here a "tag"... The tag information, along with the rest of the packet header, must accompany a packet "in the clear", that is, not encrypted" [0029]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe and Raike to include an alteration of ID data such that the altered ID data renders the type of data in the at least one stream unrecognized and partly encrypting the data segments, leaving the ID segment unencrypted as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to designate and discard certain data stream packets (Coupe [0062]) and facilitating the encryption and decryption of the data packets (Raike [0032]-[0035]).

As to Amended Claims 21 and 23:

Yamaguchi discloses a computer programme product comprising computer readable instruction for programming a processing unit (e.g. see "The present invention may be a computer system that comprises a microprocessor and memory which stores the above computer program, and the microprocessor may execute the stored computer program to achieve the present invention. The above computer program or digital signals may be

recorded on the computer-readable recording medium to be distributed via the network or other distribution methods to a computer system" [0258]), for executing the steps of,

- recognising that the data carried by the ID segment is [different from] ID data (data judging unit 117 distinguishes ID data such as a component ID from a packet ID) being pre-determined to identify the type of data in the stream of audiovisual data (e.g. see "The data judging unit 117 then compares the ID of the recognized link destination with the ID of the currently-presented presentation element to judge whether a presentation element of the link destination and the currently-presented presentation element belong to the same component" [0126]);
- forming a stream of audiovisual data from the data segments (e.g. see "The combining unit 106 receives the second AV signal from the AV reproducing unit 105, and a second data signal from the data analyzing unit 104. The combining unit 106 then combines the second AV signal and the second data signal to generate a data-AV combined signal, and outputs the generated data-AV combined signal to the monitor connected to the interactive data receiving device 100" [0108]);

But Yamaguchi does not specifically disclose:

- an alteration of ID data and the actual type of data comprised by the data segments is not recognized;
- decrypting the partly encrypted data segments (although Yamaguchi discloses "A descrambling key to descramble such scrambled AV TP [audio-video transport

packets], and program attribute information for the programs make up program information (hereafter, "ECM") and are contained in another TP (hereafter, "ECM TP"). Such ECM TP and AV TP are broadcasted together. This ECM TP is also scrambled. A work key to descramble the scrambled ECM TP, and subscription information make up individual information (hereafter, "EMM") and are stored in an integrated circuit (IC) card, which is inserted into each receiving device" [0008]);

However, the analogous art Coupe, which addresses the same field of endeavor in transmission of audio and video data packet streams, does disclose an alteration of ID data (replacement PID value [0062]) and the actual type of data comprised by the data segments is not recognized (null PID replacement value does not identify stream data as audio or video [0062] but only designates packet data to be discarded).

Furthermore, the analogous art Raike, which addresses the same field of endeavor in encryption and transmission of audio and video data streams, does disclose a decryption unit (recipient's decryption processor [0030]) for/decrypting (symmetrically decrypting [0034]) the partly encrypted data segments (encrypted stream packets with unencrypted tag values removed [0034]).

- (e.g. see Coupe, "The stream includes a transport stream packet 212, a packet header 214, and a PID 216 therein. In one embodiment, PID 216 comprises a 13-bit PID which is extracted from the packet and is to be compared to entries in a re-map table 230. In accordance with the present invention, PID re-map table 230 comprises a programmable PID look-up table having n entries, wherein in

one embodiment n=32, but in either event is less than the total of all possible PID values for a 13-bit PID. The current PID value is compared with the PID look-up entries in table 230 and if a match is found is replaced by a re-map value as indexed within the table. If no match is found, then the PID can be replaced with a null PID as shown in FIG. 6. The null PID flags the packet for discarding at a later point by the transport demultiplexor" [0062]);

- (e.g. see Raike, "The tag values of each stream data packet are extracted (13) and then hashed (14) with the base key to produce the packet key for each packet. The stream packets with tag values removed (stream data) are then symmetrically decrypted (15) using the corresponding packet key. The plaintext stream packets, with or without tag values depending on the transmission protocol being used, are then stored or outputted in a form suitable for use by a streaming media player" [0034]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the invention of Yamaguchi with the teachings of Coupe and Raike to include an alteration of ID data and the actual type of data comprised by the data segments is not recognized and a decryption unit for/decrypting the partly encrypted data segments as claimed because the use of Coupe and Raike could provide Yamaguchi the ability to partially encrypt an audio and video data stream (Yamaguchi [0008]) and replace PID values for certain data packet streams with null values (Coupe [0062]) while not encrypting the packet header segments containing the ID information (Raike [0029]) for the purpose of allowing the system to designate and

discard certain data stream packets (Coupe [0062]) and facilitating the later decryption process of the encrypted stream packets (Raike [0032]-[0035]).

5. **Claim 6** is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Coupe and Raike, as applied to claim 1 above, and in further view of Hobrock et al. (US-20040247122-A1, hereinafter Hobrock).

As to Claim 6:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 1, wherein,

- the data segments are provided with further ID data (packet ID [0065]) in the ID segment, the further ID data being pre-determined to identify the type of data in the stream of audiovisual data (e.g. see Yamaguchi, "Each packet contains a different packet ID (PID), which is identification information for the packet. A plurality of packets that has the same PID to be transmitted make up the same component" [0065])
- ID data (component ID [0066]) being different from ID data being pre-determined to identify the type of data in the at least one stream of audiovisual data (e.g. see "As shown in FIG. 2, the MPEG2 TS 200 includes components 217, 219, 201, 204, and other components that are not shown in the figure. Each component contains a different component ID that identifies the component" [0066]; see also "The component 217 includes viewing permission information 218, which contains subscription information given for each program... Video data and audio

data are included in a video data component and an audio data component, which are not shown in the figure" [0067]);

But Yamaguchi does not specifically disclose:

- the further ID data being in a further step replaced by [other] ID data.

However, the analogous art Hobrock, which addresses the same field of endeavor in encryption, decryption, and transmission of audio and video data streams, does disclose the further ID data (original PID value [0060]) being in a further step replaced by [other] ID data (new PID values [0060]).

- (e.g. see "In the interest of simplicity of encoding, a preferred embodiment of the present inventive technique accomplishes the "tagging" function by replacing each packet's PID with a new PID to identify the packet's origin transport stream. In effect, the new PID value serves a dual purpose--it serves as a "tag" value to identify the origin stream of packets in the merged stream, and it maps the original PID values into a new set of values" [0060]).

It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify the combination method of Yamaguchi, Coupe, and Raike with the teachings of Hobrock to include the further ID data being in a further step replaced by [other] ID data as claimed because the use of Hobrock could provide the combination method of Yamaguchi, Coupe, and Raike the ability to further replace original ID data in a stream of audiovisual data (Yamaguchi [0065]) with other ID data values (Hobrock [0060]) for the purpose of preventing data packet ID conflicts inside a receiving decryption device of the audiovisual data stream (Hobrock [0087]).

6. **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Coupe and Raike, as applied to claim 1 above, and in further view of Nakagawa et al. (US-20010028725-A1, hereinafter Nakagawa).

As to Claim 9:

The combination of teaching between Yamaguchi, Coupe, and Raike discloses the method according to claim 1, but does not specifically disclose further comprising the step of,

- providing an empty stream of audiovisual data of the same type as the at least one stream of audiovisual data for which non pre-determined ID data has been provided, the empty stream of audiovisual data being provided with ID data pre-determined for identifying the type of data.

However, Nakagawa does disclose providing an empty stream (If IPMPS_Type=2, payload of decoded data is cleared) of audiovisual data of the same type as the at least one stream of audiovisual data for which non pre-determined ID data has been provided, the empty stream of audiovisual data being provided with ID data (IPMP_Type) pre-determined for identifying the type of data.

- (e.g. see "On the other hand, if it is determined in step S307 that the user is not authentic (the user has not paid a given fee), the flow advances to step S308 to control playback quality of that object. In step S308, data decoded in step S305 is processed to control playback quality. How to process the data can be determined by the IPMP controller 20 depending on the format of the IPMP information" [0327]; see also "If IPMPS_Type=2, the payload of decoded data is

cleared to black out a moving image or inhibit audio playback" [0330]; see also "As described above, according to this embodiment, upon decoding and playing back information from a data stream that contains a plurality of object streams, the playback quality of copyrighted objects can be controlled" [0334])

One of ordinary skill in the art at the time applicant's invention was made would have been motivated by Nakagawa to modify the combination method of Yamaguchi, Coupe, and Raike to include providing an empty stream of audiovisual data of the same type as the at least one stream of audiovisual data for which non pre-determined ID data has been provided, the empty stream of audiovisual data being provided with ID data pre-determined for identifying the type of data as claimed because the use of Nakagawa could provide the combination method of Yamaguchi, Coupe, and Raike the ability to provide an empty stream of audiovisual data (Nakagawa [0330]) of the same type as another audiovisual data stream for which non pre-determined ID data has been provided, for the purpose of enhancing control over output data streams gained by being able to provide for an empty stream of audiovisual data for inhibiting audio or image playback to an unauthorized viewer (Nakagawa [0011]).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kubota et al. (US-6353613-B1) is cited for teaching an audio and video multiplexing system that transports and modifies PID values of data packets.

b. Unger et al. (US-20020196939-A1) is cited for teaching an encryption television program system that replaces PID values within data streams.

c. Morishita (US-20040141722-A1) is cited for teaching a video/audio apparatus that rewrites packet ID headers to nullify data stream parts.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Kenneth Chang whose telephone number is (571)270-7530. The examiner can normally be reached on Monday-Friday 8:00am-5:30pm (Alt. Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K. C./
Examiner, Art Unit 2438
04/01/10
/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438